UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,889	01/25/2002	Brian Swander	14917.0431US01	1769

27488 7590 12/08/2006

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/056,889	SWANDER ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-8,10-18,20,22 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-8,10-18,20,22 and 23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/27/06 10/3/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/27/06 has been entered.

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 3 comprises the limitation *"wherein the fragmenter module does not split the IKE data packets unless no response to a previously-sent IKE data packet has been received"*. The Applicant has not pointed out where the amended claim is supported, nor does there appear to be a written description of the claim limitation in the application as filed.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 3 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See above objection to the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3,6-8,10-18,20,22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over IPSEC, "Minutes of IPSEC Working Group Meeting", in view of Kent et al. (Kent), "Fragmentation Considered Harmful".

Regarding claim 1, IPSEC discloses changes to the IKE protocol to support network transmission (i.e. NAT/Firewall traversal) (IPSEC, page 1, #1) and the testing of the traversal of IKE packets over NAT devices, thus the *generating and transmitting an IKE packet over a network* (IPSEC, page 4, lines 1-7). IPSEC discloses that changes to the IKE protocol (to solve the IKE/NAT problem) are needed as packet fragmentation adversely affects IKE packets (IPSEC, page 4, par. 2; "Revised ESP", pars. 2, 3). IPSEC discloses as a solution that packets should be fragmented above UDP, resulting in multiple UDP packets – each packet encapsulating a fragment from the above and highest layer [application layer] where the IKE protocol stack operates (for evidence of protocol stacks, Applicant's representative may refer to the applicant's admitted Prior Art, fig. 4). Thus, IPSEC discloses *fragmenting the IKE packet into a plurality of smaller packets* and *transmitting each of the plurality of smaller packets over a network* (IPSEC, page 4, lines 1-7).

IPSEC discloses that IKE packets should be fragmented before the UDP layer. However, IPSEC does not disclose specifically methods packet fragmentation, such as conditions requiring fragmentation and that a packet fragment should have a proper packet header.

Kent et al. discloses principles for packet fragmentation. While Kent discusses these principals of packet fragmentation often in the context of the IP layer (Kent, pg. 75, par. 4), Kent further discloses that these fragmentation methods are to be applied in higher protocol layers as well. Upper level protocol layers should be cognizant of

fragmentation issues, and should fragment or send smaller packet sizes if the it is known that a larger packet size will be fragmented at the IP layer (Kent et al., section 3, par. 4). For example, Kent discloses that an upper layer (i.e. TCP) should not send a large un-fragmented segment when it a lower layer (i.e. IP) will have to fragment it (Kent, pg. 79, pars. 3, 4).

Kent discloses that the packet fragmentation method consists of fragmenting a larger packet into a plurality of fragments. Each fragment is sent as a separate packet, with each of the plurality of smaller packets containing a properly formatted header according to the protocol (Kent et al., section 2.1).

It would have been obvious to one of ordinary skill in the art to employ the principles for packet fragmentation disclosed by Kent with the teachings of IPSEC requiring the fragmentation of IKE packets above the UDP layer. This would have been obvious because one of ordinary skill in the art would have been motivated to practically implement packet fragmentation methods for the purpose of fragmenting IKE packets above the UDP layer as required by IPSEC, so that the packets would not be improperly fragmented at the IP layer. The combination of IPSEC and Kent discloses that fragmented packets each have a proper header, and thus, it would have been obvious to one of ordinary skill in the art to follow this teaching as required by the combination of IPSEC and Kent when fragmenting IKE messages before they are passed to the UDP layer.

Therefore, the combination of IPSEC and Kent et al. discloses:

determining whether a response to the IKE packet was received and *fragmenting the IKE packet into a plurality of smaller packets when a response is not received* (Kent et al., section 3.3, pars. 1 - 3). To avoid improper fragmentation at the IP layer, the combination of IPSEC and Kent et al. discloses that a transmitting host would choose whether to fragment an IKE packet using received acknowledgements ("a response") of successful packet transmission. If the host does not receive an acknowledgment ("a response") then it will have to fragment it's transmitted packets into smaller packets until it receives a successful transmission acknowledgment, and accordingly discovers the proper fragment length for transmitting packets.

Regarding claim 2, the combination of IPSEC and Kent et al. discloses:

wherein each header includes an identifier that may be used to associate the smaller packet with a corresponding IKE packet (Kent et al., section 2, par. 4, lines 1-8; section 2.1, par. 2)

Regarding claim 3, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of IPSEC and Kent et al. discloses:

a User Datagram Protocol (UDP) stack that is capable of generating UDP data packets for transmission over a network (IPSEC; page 4, lines 1-8). IPSEC discloses the generation of multiple UDP packets and the fragmentation of IKE packets above UDP (thus, a UDP stack) for network transmission;

an IKE protocol stack that generates IKE data packets that are subsequently processed by the UDP protocol stack (IPSEC; page 4, lines 1-8). IPSEC discloses the generation and fragmentation of IKE packets (thus an IKE stack). The packets pass from a layer above UDP to a layer below UDP, and are fragmented above the UDP layer.

and a fragmenter module that intercepts IKE data packets prior to being processed by to the UDP protocol stack and splits the IKE data packets into a plurality of smaller data packets that may be subsequently formatted by the UDP protocol stack (IPSEC, page 4, lines 1-8). IPSEC discloses fragmenting IKE packets (thus a fragmenter module) in a layer above the UDP layer (thus intercepting IKE packets prior to being processed by the UDP stack).

wherein the fragmenter module does not split the IKE data packets unless no response to a previously-sent IKE data packet has been received (Kent et al., section 3.3, pars. 1 – 3). Herein, the combination discloses that once a suitable response is received, the fragmenter module does not continue to split the data packets.

and wherein, each of the plurality of smaller data packets includes a header formatted according to the IKE protocol (see rejection of claim 1).

Regarding claim 6, the combination of IPSEC and Kent et al. disclose:

receiving a plurality of fragments of an IKE data packet from a transmitting node, wherein each fragment includes an identifier that associates each fragment with an IKE

data packet ; and discarding all fragments that contain a first identifier if a predetermined number of fragments are received that contain a second identifier (Kent et al., section 2.4, par. 3);

and determining the total size of all fragments that contain the same identifier and discarding said fragements when the total size exceeds a predetermined limit (Kent et al., section 2.4, par. 2, 3). Herein, the combination discloses that a fragment reassembly process may not progress if the total size of a datagram (comprising fragments with a same identifier) exceeds a predetermined limit. As an example, a sufficiently sized space for reassembling a large datagram could comprise a size of 8 buffer spaces. Thus, when that predetermined limit is achieved, the occupying fragments of an unassembled datagram will expire and be discarded.

Regarding claim 7, the combination of IPSEC and Kent et al. disclose:

wherein the step of discarding all fragments that contain a first identifier is performed when at least one fragment is received that contains a second identifier (Kent et al., section 2.4, par. 3).

Regarding claim 8, the combination of IPSEC and Kent et al. disclose:

determining whether all fragments that are associated with an IKE data packet have been received, and sending a no acknowledgment (NAK) message to the transmitting node when at least one fragment has not been received (Kent et al., section 3.3.3). A receiving host is disclosed as making a determination as to whether all

fragments associated with an IKE packet has been received. The receiving host will convey a "Time exceeded" message ("NAK") to the transmitting host when at least one fragment has not arrived, indicating to the transmitting host that it has not received all the fragments.

Regarding claim 10, the combination of IPSEC and Kent et al. does not disclose *wherein the predetermined limit is 64 kilobytes*. This, however, would have been obvious to one of ordinary skill in the art to set a predetermined limit of 64 kilobytes as the total size of all possible fragments. As evidenced by the "Glossary for the Linux FreeS/WAN project" – (definition for DoS), this would have been obvious to one of ordinary skill in the art because the standardized size limit of an IP packet is 64 kilobytes, and a failure to discard illegitimate packets when the size exceeds the standard limit would result in denial of service attacks.

Regarding claim 11, it is rejected, at least, for the same reasons provided for the rejection of claims 1 and 2, and furthermore because the combination discloses that to avoid unnecessary fragmentation of packets (Kent, section 3.2), the system should be cognizant of network timing issues. Thus, a system will not assume it is necessary to retransmit a packet until a determined period of time ("round-trip time" or the estimated time period between a sender's packet transmission and a sender's reception of a packet acknowledgement response)(Kent, section 3.2.1).

While the combination does not nominally recite "a timer", it would have been obvious to one of ordinary skill in the art to employ appropriate timing means ("a timer") for determining when packet retransmission is necessary. This would have been obvious because one of ordinary skill in art would have been motivated by the combination's teachings for measuring and determining timing delays before retransmitting previously transmitted packets within a system.

Regarding claim 12, the combination of IPSEC and Kent et al. disclose:

further comprising means for determining the capability of the receiver node for receiving fragmented packets (Kent et al., section 3.3, par. 2).

Regarding claims 13, 14, and 15 they are rejected, at least, for the same reasons as claims 1 and 2.

Regarding claim 16, the combination of IPSEC and Kent et al. disclose:

wherein the plurality of smaller packets contain the same information as that contained within the original IKE packet (Kent et al., section 2.4, par. 3, section 2.1).

Regarding claim 17, the combination of IPSEC and Kent et al. disclose:

wherein at least one of the plurality of smaller packets contains the header formatted according to the IKE protocol (Kent et al., section 2.1). As disclosed by the combination of IPSEC and Kent et al., fragmentation involves fragmenting the original

packet into smaller packets, each containing the protocol and header fields of the original packet.

Regarding claim 18, it is rejected, at least, for the same reasons as claims 1 and 11, and furthermore because the combination of IPSEC and Kent discloses:

wherein the steps of generating, determining and fragmenting are performed independently of performing any steps on the data packet corresponding to a transport layer protocol and/or a network layer protocol (IPSEC, page 4, lines 6-8). The combination of IPSEC and Kent discloses generating and fragmentation (accordingly determination to fragment) as occurring before the lower protocol layers.

Regarding claim 20, it is rejected, at least, for the same reasons as claims 1 and 11, and further because the combination of IPSEC and Kent et al. disclose:

fragmenting the packet into a plurality of fragments using a code module that does not implement the TCP, UDP or IP protocols before the packet is processed by a code module that does implement the TCP, UDP or IP protocols (IPSEC; page 4, lines 1-8; Kent et al., section 3). The combination of IPSEC and Kent et al. disclose the fragmentation of IKE packets above the UDP layer - this would include TCP (parallel to UDP) and IP (below UDP). The fragmentation is computer based and therefore inherently performed by some type of module for instructing a computer ("code module").

comprising including an identifier that identifies the data packet in eah packet fragment (see rejection of claim 2); *and transmitting the packet fragments over a network* (see rejection of claim 1).

Claims 22 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of IPSEC and Kent in view of Cerf et al. (Cerf), "A Protocol for Packet Network Intercommunication".

Regarding claim 22, the combination of IPSEC and Kent et al. disclose:

receiving a plurality of fragments of a single IKE data packet, wherein the fragments were transmitted from a transmitting node in an order that can be determined from information contained within the received data fragments (Kent et al.; section 2.1, par. 3; section 2.4, par. 3). The combination does not disclose that a receiver may detect duplicate packets from a single IKE packet and then discard such duplicates.

Cerf discloses that a receiver which receives duplicate packets will discard such duplicates. Additionally, Cerf discloses that a receiver may detect out of order packets, and choose to store and acknowledge such packets or discard such packets (Cerf, pg. 7-8, "Retransmission and Duplicate Detection"). It would have been obvious to one of ordinary skill in the art to detect and discard duplicate packets. This would have been obvious because one of ordinary skill in the art would have been motivated to avoid resource consummation by superfluous data.

Regarding claim 23, the combination discloses *sending a message to the transmitting node that out of order packets have been received* (Cerf, pg. 7-8, "Retransmission and Duplicate Detection").

Response to Arguments

Applicant's arguments filed 9/25/06 have been fully considered but they are not persuasive.

Applicant's representative argues primarily that:

(i) *Neither IPSEC nor Kent, nor their combination, teaches or suggests using the absence of a response to an IKE packet to determine whether to fragment IKE packets.* (Remarks, pg. 8)

In response, the examiner finds the arguments of the applicant's representative to be unpersuasive. The prior art combination does in fact disclose that a transmitter will continue to fragment a transmitted datagram until a response is received from a receiver informing the transmitter that the data has been properly received (applicant are respectfully encouraged to review the prior art references and the rejection of claim 1).

(ii) *Kent does not teach or suggest determining the total size of all fragments that contain the same identifier, nor does it teach or suggest discarding said fragments when the total size exceeds a predetermined limit. IPSEC does not remedy this deficiency in Kent.* (Remarks, pg. 9)

In response, the examiner finds the arguments of the applicant's representative to be unpersuasive. The prior art combination does in fact disclose determining a total size of assembled fragments and the discarding of fragments when a total size exceeds a predetermined limit (unassembled fragments whose total size exceeds the limit will expire and be discarded). The examiner respectfully encourages the applicant to review the prior art references and the rejection of claim 6.

The examiner notes that other arguments by the applicant are essentially similar to the ones above and are new arguments directed towards new/amended limitations.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffery Williams
AU: 2137

JW

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER